# Biometric Data Privacy Liability Increasing Sharply

Business Bulletin

Processing of biometric data is a hot topic in privacy law right now, and has rapidly become a sharply increasing source of claims for cyber liability insurers. A leading cause of this spike has been the hundreds of consumer lawsuits brought over suspected violations of the Illinois Biometric Information Privacy Act, or BIPA. Organizations that are collecting, using and sharing biometric data need to be aware of the potential liabilities involved.

BIPA was passed into law in Illinois in 2008 with the goal of protecting the privacy of biometric information collected from consumers and employees, and to establish standards of conduct for the entities that collect and store such data. Class action litigation under this law has been emboldened in the wake of the IL Supreme Court's decision in January, 2019 in *Rosenbach v. Six Flags Entm't Corp.*, in which it was determined that in order to collect damages, a plaintiff did not have to prove that they were injured by an improper collection of their biometric data, only that such a violation occurred.

While BIPA itself is an Illinois state law, it is worth noting that at least a dozen other states have or are considering similar laws. Furthermore, many additional states include biometric data in their definition of personal information protected by their overall consumer privacy laws, and as those familiar with this arena can attest, the specifics of these laws vary substantially from jurisdiction to jurisdiction. For example, did you know that the new California Consumer Privacy Act (CCPA) specifically includes not only records commonly considered to be biometric data such as fingerprints and retinal scans, but also things such as walking gait and keystroke patterns, as protected private information?

Companies collecting biometric data, whether for relatively standard HR purposes such as time clocks or for more detailed identity recognition purposes, should evaluate their exposure in this area. Included in the review should be an examination of policies and procedures for accessing, using, processing, storing, disclosing, and deleting biometric information, as well as obtaining consent where necessary. An additional examination should include whether you are comfortable that your third party service or cloud provider is compliant and capable of safeguarding the data.

Many of these liability exposures are insurable through properly constructed employment practices liability programs or cyber liability programs or a combination of both. The experts at Simkiss & Block can help you manage these needs, so contact us to get started.